Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listinq of Claims:

1. (canceled)

2. (original) The apparatus of claim 74, further comprising:

a thread count storage to store a thread count indicating a number of threads currently initialized for operation in the isolated execution mode.

3. (original) The apparatus of claim 74, further comprising:

an identifier log storage to store a cryptographic identifier of an executive entity loaded into the isolated execution mode.

4. (original) The apparatus of claim 74, further comprising:

a platform key storage to store a platform key used in handling an executive entity loaded into the isolated execution mode; and

a scratch storage to store isolated settings used to configure the isolated execution mode.

5. (original) The apparatus of claim 3, wherein the executive entity comprises at least one entity selected from the group consisting of a PE, a PE handler, and an operating system executive (OSE).

6. (original) The apparatus of claim 74, further comprising:

a chipset circuit that provides the PE handler storage and the initialization storage, the chipset circuit capable of supporting at least one chipset mode selected from the group consisting of:

an initialization waiting mode to indicate the chipset circuit is waiting for initialization;

a PE initialization in-progress mode to indicate the PE is being executed;

a PE initialization completion mode to indicate the PE is completed;

an OSE loaded mode to indicate the OSE has been loaded; and

a closing mode to indicate the isolated execution mode is closed.

7. (canceled)

8. (original) The apparatus of claim 74, wherein the initialization storage returns an incremented thread count when a thread enrolls in the isolated execution mode and returns a decremented thread count when an enrolled thread withdraws from the isolated execution mode.

9. (original) The apparatus of claim 74, further comprising a mode write circuit to write a failure mode into the chipset circuit when a thread limit is reached.

10. (original) The apparatus of claim 74, the PE handler storage further to store at least one item selected from the group consisting of a cryptographic PE handler identifier, a PE handler size, and a PE handler address.

11. (original) The apparatus of claim 74, wherein the PE handler storage comprises a read-only memory.

12. (original) The apparatus of claim 74, further comprising a platform key storage to return a platform key when the chipset circuit is read in an initialization waiting mode.

13. (original) The apparatus of claim 12 wherein the platform key is programmed to a random value.

14. (original) The apparatus of claim 74, further comprising:

a status storage to store a status value of an isolated unlock pin used in setting platform settings.

15. (original) The apparatus of claim 4 wherein the isolated settings comprise one or more values selected from the group consisting of an isolated base value for the isolated memory area, an isolated length value for the isolated memory area, and a processor executive entry address.

16. (canceled)

17. (original) The method of claim 75, further comprising:

storing a thread count in a thread count storage indicating number of threads currently initialized for operation in the isolated execution mode.

18. (original) The method of claim 75, further comprising:

storing cryptographic identifiers of executive entities loaded into the isolated execution mode.

19. (original) The method of claim 75, further comprising:

obtaining a platform key used in handling the executive entities ~~in~~ from a platform key storage; and

obtaining isolated settings used to configure the isolated execution mode from the chipset circuit.

20. (original) The method of claim 18, wherein the executive entities comprise at least one entity selected from the group consisting of a PE, a PE handler, and an operating system executive (OSE).

21. (original) The method of claim 75, further comprising operating in a series of chipset modes comprising:

an initialization waiting mode to indicate the chipset circuit is waiting for initialization;

a PE initialization in-progress mode to indicate the PE is being executed;

a PE initialization completion mode to indicate the PE is completed;

an OSE loaded mode to indicate the OSE has been loaded; and

a closing mode to indicate the isolated execution mode is closed.

22. (original) The method of claim 75, further comprising initializing at least a portion of the chipset circuit.

23. (original) The method of claim 75, further comprising:

returning an incremented thread count when a thread enrolls in the isolated execution mode; and

returning a decremented thread count when an enrolled thread withdraws from the isolated execution mode.

24. (original) The method of claim 75, further comprising writing a chipset mode corresponding to a failure mode when a thread count reaches a thread limit.

25. (canceled)

26. (original) The method of claim 75, wherein the PE handler storage comprises read-only memory.

27. (original) The method of claim 75, further comprising obtaining a platform key from a platform key storage when the chipset circuit is in an initialization waiting mode.

28. (canceled)

29. (original) The method of claim 75, further comprising:

storing a status value of an isolated unlock pin used to unlock platform settings.

30. (original) The method of claim 19 wherein the operation of obtaining isolated settings comprises obtaining at least one value selected from the group consisting of an isolated base value for the isolated memory area, an isolated length value for the isolated memory area, and a processor executive entry address.

31-46. (canceled)

47. (original) The system of claim 61 wherein the chipset circuit further comprises:

a thread count storage to store a thread count indicating a number of threads currently associated with the isolated execution mode.

48. (original) The system of claim 61 wherein the chipset circuit further comprises:

an identifier log storage to store cryptographic identifiers of executive entities associated with the isolated execution mode.

49. (original) The system of claim 61 wherein the chipset circuit further comprises:

a platform key storage to store a platform key used in handling executive entities; and

a scratch storage to store isolated settings used to configure the isolated execution mode.

50. (original) The system of claim 48 wherein the executive entities comprise:

a processor executive (PE);

a PE handler; and

an operating system executive (OSE).

51. (original) The system of claim 61 wherein the chipset circuit further comprises a mode storage to store a chipset mode indicating a mode of operation of the chipset circuit, the chipset mode comprising one or more modes selected from the group consisting of:

an initialization waiting mode to indicate the chipset circuit is waiting for initialization;

a PE initialization in-progress mode to indicate the PE is being executed;

a PE initialization completion mode to indicate the PE is completed;

an OSE loaded mode to indicate the OSE has been loaded; and

a closing mode to indicate the isolated execution mode is closed.

52. (canceled)

53. (original) The system of claim 61 wherein the chipset circuit further comprises an initialization storage to return an incremented thread count when a thread enrolls in the isolated execution mode, and to return a decremented thread count when an enrolled thread withdraws from the isolated execution mode.

54. (original) The system of claim 51 wherein the chipset circuit further comprises a mode write circuit to write a failure mode into the mode storage when a thread limit is reached.

55. (original) The system of claim 61, the PE handler storage further to store at least one item selected from the group consisting of a PE handler cryptographic identifier, a PE handler size, and a PE handler address.

56. (original) The system of claim 61 wherein the PE handler storage comprises a non-volatile memory.

57. (original) The system of claim 49 wherein the platform key is returned when the platform key storage is read with the chipset circuit in an initialization waiting mode.

58. (original) The system of claim 49 wherein the platform key comprises a random value.

59. (original) The system of claim 61 wherein the chipset circuit further comprises:

a status storage to store a status value of an isolated unlock pin used to unlock platform settings.

60. (original) The system of claim 49 wherein the isolated settings comprise one or more values selected from the group consisting of an isolated base value for the isolated memory area, an isolated length value for the isolated memory area, and a processor executive entry address.

61. (currently amended) A system comprising:

a processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode;

a memory to include an isolated memory area accessible to the processor in the isolated execution mode;

a chipset circuit in communication with the processor and the memory; and

a ~~PE~~ processor executive (PE) handler storage in the chipset circuit, the PE handler storage to store a PE handler image to be loaded into the isolated memory area after at least a portion of the chipset circuit is initialized.

62. (original) An apparatus comprising:

a machine accessible medium; and

instructions encoded in the machine accessible medium, wherein the instructions, when executed by a processing system with a processor and a chipset circuit that supports a normal execution mode and an isolated execution mode, cause the processing system to perform operations comprising:

obtaining a processor executive (PE) handler image from a PE handler storage in the chipset circuit; and

after at least a portion of the chipset circuit is initialized, loading the PE handler image into an isolated memory area within a memory of the processing system, the isolated memory area accessible to the processor in the isolated execution mode.

63. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to store a thread count indicating number of threads currently initialized for operation in the isolated execution mode.

64. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to store cryptographic identifiers of executive entities loaded into the isolated execution mode.

65. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to store a platform key used in handling executive entities.

66. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to configure the isolated execution mode, based at least in part on isolated settings associated with the processing system.

67. (original) The apparatus of claim 66, wherein the isolated settings include at least one value selected from the group consisting of an isolated base value for the isolated memory area, an isolated length value for the isolated memory area, and a processor executive entry address.

68. (original) The apparatus of claim 62, wherein the instructions implement executive entities comprising at least one entity selected from the group consisting of:

a PE;

a PE handler; and

an operating system executive (OSE).

69. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to initialize at least a portion of the chipset circuit.

70. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises:

instructions to increment a thread count when a thread enrolls in the isolated execution mode; and

instructions to decrement a thread count when an enrolled thread withdraws from the isolated execution mode.

71. (original) The apparatus of claim 62, wherein the instructions obtain the PE handler image from a read-only memory.

72. (original) The apparatus of claim 62, wherein the instructions obtain a platform key from a platform key storage when the chipset circuit is in an initialization waiting mode.

73. (original) The apparatus of claim 62, wherein the machine accessible medium further comprises instructions to store a status value of an isolated unlock pin used to unlock platform settings.

74. (currently amended) An apparatus comprising:

a ~~PE~~ processor executive (PE) handler storage to store a PE handler image to be loaded into an isolated memory area within a memory of a processing system after at least a portion of a chipset circuit of the processing system is initialized, the PE handler image to be executed by a processor of the processing system, the processor capable of operating in a normal execution mode and in an isolated execution mode; and

an initialization storage to configure the processing system in the isolated execution mode, the processor capable of accessing the isolated memory area when operating in the isolated execution mode.

75. (original) A method comprising:

storing a processor executive (PE) handler image in a PE handler storage of a chipset circuit, the chipset circuit in communication with a processor that supports a normal execution mode and an isolated execution mode, and in communication with a memory to include an isolated memory area accessible to the processor in the isolated execution mode; and

after at least a portion of the chipset circuit is initialized, loading the PE handler image into the isolated memory area.